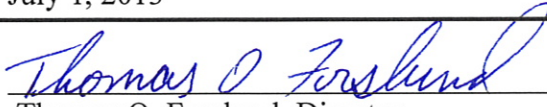
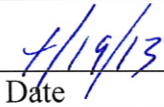


Thomas O. Forslund, Director

Governor Matthew H. Mead

<b>Policy Title:</b>	Assigned Privacy/Security Responsibility	
<b>Policy Number:</b>	S-002	
<b>Effective Date:</b>	July 1, 2013	
<b>Approval:</b>	 Thomas O. Forslund, Director	 Date

**Purpose:**

This policy establishes the Wyoming Department of Health's (WDH) responsibility to designate both an internal Privacy/Compliance Officer and a Security Officer to facilitate the implementation and oversight of activities relating to the privacy and security of protected health information (PHI) and electronic protected health information (ePHI).

**Policy:****1. Assigned Privacy/Compliance Responsibility**

WDH shall designate a Privacy/Compliance Officer to provide guidance and oversight regarding the collection, maintenance, use and dissemination of PHI. The Privacy/Compliance Officer shall oversee all activities related to the development, implementation, maintenance of, and adherence to the Agency's privacy and security policies, procedures and practices.

**2. Identification****a. The WDH Privacy/Compliance Officer is:**

De Anna Greene, CIPP, CIPP/G, CIPP/IT  
(307)777-8664 office  
(307)777-7439 fax  
2300 Capitol Ave., 4<sup>th</sup> Floor  
Cheyenne, WY 82002  
[deanna.greene@wyo.gov](mailto:deanna.greene@wyo.gov)

**b. The backup WDH Privacy/Compliance Officer is:**

Lee Clabots, M.P.H.  
WDH Deputy Director  
(307)777-5759 office  
(307)777-7439 fax  
2300 Capitol Ave., 4<sup>th</sup> Floor  
Cheyenne, WY 82002  
[lee.clabots@wyo.gov](mailto:lee.clabots@wyo.gov)

**3. Responsibilities of the WDH Privacy/Compliance Officer**

- a. Works with WDH Senior Management to establish and implement agency-wide privacy policies and procedures.
- b. Provides information regarding WDH's privacy practices. Responsible for receiving, responding to, and documenting complaints. Responsible for conducting thorough and timely investigations of all complaints lodged against WDH. Determines the viability and severity

- of complaints and coordinates corrective action, mitigation, and disciplinary action collaboratively with the WDH Security Officer, Senior Management, and Human Resources, the Attorney General, and other appropriate persons and/or offices.
- c. Annually assesses the performance of WDH workforce responsible for privacy and security oversight, training programs, etc.; analyzes whether any gaps exist; and determines timeframes and resources necessary to address the identified gaps. Biannually (every other year) performs a privacy risk assessment of WDH policies and procedures.
  - d. Works with the Attorney General's Office and WDH workforce to ensure WDH maintains appropriate privacy and confidentiality consents, authorization forms, information notices and materials reflecting current practices and requirements.
  - e. Prepares annual report(s) to WDH Senior Management advising of future requirements necessary to maintain compliance.
  - f. Oversees and directs training on privacy and security policies and procedures to all WDH workforce members and other appropriate parties, as necessary.
  - g. Maintains documentation to demonstrate required training has been administered in a timely manner.
  - h. Works with the WDH Public Information and Security Officers to initiate, facilitate, and promote activities which foster information privacy/security awareness within WDH.
  - i. Ensures all members of the WDH workforce are informed when policies and procedures are changed or updated.
  - j. Evaluates adherence to WDH's privacy and security policies and procedures by all WDH divisions/programs/facilities and workforce. Conducts ongoing compliance monitoring activities.
  - k. Initiates and conducts an internal privacy audit program.
  - l. Establishes, with the WDH Security Officer, access tracking mechanisms to track electronic accesses of ePHI to gauge appropriate role-based access, appropriate activity, and to provide requested access reports to clients.
  - m. Works cooperatively with other agencies to respond appropriately to patient requests to inspect, amend, and restrict access to PHI.
  - n. Establishes a process for receiving, documenting, tracking, investigating, and taking corrective action on all complaints concerning the WDH privacy and security policies and procedures (including self-disclosures).
  - o. Collaborates with WDH Human Resources and Administration and the Attorney General to develop appropriate sanctions addressing failure to comply with privacy and security policies and procedures.
  - p. In conjunction with the appropriate WDH office (e.g., Human Resources), applies sanctions consistently to all WDH workforce members, extended workforce, and business associates.
  - q. Implements corrective action(s) to mitigate effects of inappropriate use or disclosure of PHI and documents such actions.
  - r. Works collaboratively with the Attorney General's Office to identify business associates and implement business associate agreements. Reviews and evaluates proposed business associate agreements and other documents to identify and correct potential conflicts between WDH's privacy policies and procedures and applicable federal and state laws and regulations.

- s. Serves as a liaison to, and cooperates with, the U.S. Department of Health and Human Services, Office for Civil Rights, and other legal entities for compliance reviews or investigations.
  - t. Sets and tracks compliance measures, which may include:
    - i. The number of breach of confidentiality/impermissible disclosure-related complaints;
    - ii. The number of claims alleging confidentiality/privacy incidents;
    - iii. Regulatory fines related to confidentiality/privacy issues;
    - iv. The number of internal incidents involving violations of privacy policies; and
    - v. Percentage of WDH workforce members receiving timely privacy training.
  - u. Serves as a liaison to the WDH Institutional Review Board.
  - v. Reviews all information security plans for WDH systems that maintain PHI throughout the Agency/Enterprise network to ensure alignment between security and privacy practices.
  - w. In the event that the WDH Privacy/Compliance Officer needs to be replaced, the backup WDH Privacy/Compliance Officer shall serve as the interim WDH Privacy/Compliance Officer until a new WDH Privacy/Compliance Officer is selected. The search for a new WDH Privacy/Compliance Officer shall be conducted expeditiously, and the final selection shall be made by the WDH Deputy Director.
  - x. All workforce members shall be apprised of the WDH Privacy/Compliance Officer's identity, role and responsibilities. Any WDH Privacy/Compliance Officer changes shall be promptly communicated.
- 4. Assigned Security Responsibility**
- WDH shall designate a Security Officer to provide guidance and oversight regarding the creation, receipt, maintenance and transmission of ePHI. The WDH Security Officer shall develop and implement policies and procedures to ensure the confidentiality, integrity, and availability of ePHI and to protect against threats or hazards to the security or integrity of such information.
- 5. Identification**
- a. The WDH Security Officer is:  
 Tate Nuckols, JD  
 (307)777-2438 office  
 (307)777-7439 fax  
 2300 Capitol Ave., 4<sup>th</sup> Floor  
 Cheyenne, WY 82002  
[tate.nuckols@wyo.gov](mailto:tate.nuckols@wyo.gov)
  - b. The backup WDH Security Officer is:  
 De Anna Greene, CIPP, CIPP/G, CIPP/IT  
 WDH Privacy/Compliance Officer  
 (307)777-8664 office  
 (307)777-7439 fax  
 2300 Capitol Ave, 4<sup>th</sup> Floor  
 Cheyenne, WY 82002  
[deanna.greene@wyo.gov](mailto:deanna.greene@wyo.gov)
- 6. Responsibilities of the Security Officer**
- a. Spearheads the development and enforcement of information security policies and procedures, measures and mechanisms to ensure the prevention, detection, containment,



- and correction of security incidents. Ensures security standards comply with statutory and regulatory requirements regarding ePHI.
- b. Maintains security policies that include:
    - i. Administrative security: Formal mechanisms for risk analysis and management, information access controls, and appropriate sanctions for failure to comply.
    - ii. Workforce security: Formal mechanisms for ensuring role-based access (i.e., WDH workforce have access to only sensitive information necessary to perform their job duties).
    - iii. Physical safeguards: Ensure assigned security responsibilities, control access to media (e.g., compact disks, Universal Serial Bus (USB), tapes, backups, disposal of data), protect against hazards and unauthorized access to computer systems, and secure workstation locations and use.
    - iv. Technical security: Establish access controls, emergency procedures, authorization controls, and data/entity access and authentication.
  - c. Provides leadership in creating and implementing an agency-wide security program.
  - d. Ensures processes are implemented to comply with federal and state laws related to privacy, security, confidentiality, protection of information resources and health care information.
  - e. Develops, implements and administers agency-wide authorization procedures for access to, use and disclosure of ePHI.
  - f. Develops, implements and administers agency-wide procedures to ensure appropriate response to individuals exercising their rights under applicable state and federal laws.
  - g. Receives and investigates complaint allegations (e.g., non-compliance, unauthorized or inappropriate releases of PHI and ePHI), mitigates appropriately, and provides information relating to WDH's privacy and security programs.
  - h. Establishes reporting channels for suspected incidents and/or complaints.
  - i. Maintains security procedures that include:
    - i. Evaluation of compliance with security measures;
    - ii. Contingency plans for emergencies and disaster recovery;
    - iii. Security incident response process and protocols;
    - iv. Testing and enhancement of security procedures, measures, and mechanisms; and
    - v. Security incident reporting mechanisms and sanction policy.
  - j. Maintains appropriate security measures and mechanisms that guard against both unauthorized access to electronically stored and/or transmitted patient data and reasonably anticipated threats and/or hazards, including:
    - i. Integrity controls;
    - ii. Authentication controls;
    - iii. Access controls;
    - iv. Encryption; and
    - v. Abnormal condition alarms, audit trails, entity authentication and event reporting.
  - k. Oversees and ensures continuous security monitoring of information systems, including:
    - i. Performing periodic information security risk assessments;
    - ii. Conducting functionality and gap analysis, risk assessments and other system testing to determine the extent to which key business activities and infrastructure comply with statutory and regulatory requirements; and

- iii. Evaluating and recommending new information security technologies and counter-measures against threats to information, privacy or security.
- l. Ensures compliance through adequate training, awareness programs and security audits.
- m. Serves as a resource regarding matters of information security and reports the status of information security to the WDH Privacy/Compliance Officer.

**Contacts:**

De Anna Greene, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer (307) 777-8664  
Tate Nuckols, JD, WDH Security Officer (307)777-2438

**Policies:**

**References:**

45 CFR § 164.308(a)(2)  
45 CFR § 164.530(a)(1)(i) and (ii) and (2)

**Training:**